WHAT IS CLAIMED IS:

1. A wireless adhoc communication system formed of a plurality of terminals, said wireless adhoc communication system comprising:

a first terminal for transmitting a frame in which an authentication header is given; and

a second terminal for receiving said frame and confirming that said authentication header is valid,

wherein said first terminal generates said authentication header by using an authentication header key with respect to said second terminal, and said second terminal confirms that said authentication header is valid by using said authentication header key.

2. A wireless adhoc communication system formed of a plurality of terminals, said wireless adhoc communication system comprising:

a first terminal for encrypting the payload of a first frame and transmitting the first frame in which a first authentication header is given;

a second terminal for receiving said first frame and transmitting a second frame containing said encrypted payload, in which a second authentication header is given when it is confirmed that said first authentication header

is valid; and

a third terminal for receiving said second frame and decrypting said encrypted payload when it is confirmed that said second authentication header is valid,

wherein said first terminal encrypts said payload by using an encryption key with respect to said third terminal, and generates said first authentication header by using said first authentication header with respect to said second terminal,

said second terminal confirms that said first authentication header is valid by using said first authentication header and generates said second authentication header by using said second authentication header with respect to said third terminal, and

said third terminal confirms that said second authentication header is valid by using said second authentication header key and decrypts said payload by using said encryption key with respect to said first terminal.

3. A terminal comprising:

a key management list table having at least one key management list in which authentication header keys with respect to other terminals are held in such a manner as to correspond to the terminal identifiers of said other terminals;

means for searching said key management list for said key management list containing the transmission terminal identifier of a received frame in order to extract said corresponding authentication header key; and

means for confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key.

4. A terminal according to Claim 3, further comprising:

a path table having at least one path list for holding a transfer destination terminal identifier for causing a frame to arrive at another terminal in such a manner as to correspond to the terminal identifier of the other terminal; and

means for searching said path table for said path list containing an end-point terminal identifier and transmitting said frame to said transfer destination terminal identifier when said authentication header is valid and the end-point terminal identifier of said frame is not the terminal identifier of the other terminal and for discarding said frame when said authentication header is not valid.

5. A terminal comprising:

a key management list table having at least one key

management list for holding an authentication header key and a unicast encryption key with respect to another terminal in such a manner as to correspond to the terminal identifier of said other terminal;

means for searching said key management list table for said key management list containing the transmission terminal identifier of a received frame in order to extract said corresponding authentication header key;

means for confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key;

means for searching said key management list table for said key management list containing a start-point terminal identifier of said frame in order to extract said corresponding unicast encryption key when said authentication header is valid and the end-point terminal identifier of said frame is the terminal identifier of the other terminal; and

means for decrypting the payload of said frame by using said extracted unicast encryption key.

6. A terminal comprising:

a key management list table having at least one key management list for holding an authentication header key with respect to another terminal in such a manner as to

correspond to the terminal identifier of said other terminal;

means for searching said key management list table for said key management list containing the reception terminal identifier of a frame to be transmitted in order to generate an authentication header by using said corresponding authentication header key and for giving the authentication header to said frame; and

means for transmitting said frame.

7. A terminal comprising:

a key management list table having at least one key management list for holding authentication header keys and unicast encryption keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of said other terminals;

means for searching said key management list table for said key management list containing the reception terminal identifier of a frame to be transmitted in order to generate an authentication header by using said corresponding authentication header key and for giving the authentication header to said frame;

means for searching said key management list table for said key management list containing the end-point terminal identifier of said frame and for encrypting the payload of

said frame by using said corresponding unicast encryption key; and

means for transmitting said frame.

8. A terminal comprising:

a neighboring terminal list table for holding the terminal identifier of another terminal with which direct communication is possible among the terminals which form a network;

a key management list table having at least one key management list for holding an authentication header key with respect to another terminal in such a manner as to correspond to the terminal identifier of the other terminal which forms said network; and

means for, when a leaving from said network occurs at the terminals whose terminal identifiers are held in said neighboring terminal list table, deleting from said key management list table said key management list containing the terminal identifier of the terminal that has left the network.

9. A terminal according to Claim 8, further comprising means for transmitting a terminal leaving message for informing the terminal identifier of said terminal that has left the network to the other terminals which form said

network in a case where the terminal whose terminal identifier is held in said neighboring terminal list table leaves the network.

10. A terminal comprising:

a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of the other terminals which form a network; and

means for, when a terminal leaving message informing the terminal identifier of the terminal which has left said network is received, deleting from said key management list table said key management list containing the terminal identifier of the terminal that has left the network.

11. An authentication method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of said other terminals, said authentication method comprising the steps of:

searching said key management list table for said key management list containing the transmission terminal identifier of a received frame in order to extract said

authentication header key; and

confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key.

12. An authentication method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of said other terminals, said authentication method comprising the steps of:

searching said key management list table for said key management list containing the transmission terminal identifier of a received frame in order to extract said authentication header key;

generating a keyed hashed value, in which said extracted authentication header key is hashed together with a predetermined area of said frame; and

confirming whether or not said authentication header is valid by comparing said keyed hashed value with the authentication header of said frame.

13. An encryption method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys and

unicast encryption keys with respect to other terminals in such a manner as to correspond to the terminal identifiers of said other terminals, said encryption method comprising the steps of:

searching said key management list table for said key management list containing the transmission terminal identifier of a received frame in order to extract said authentication header key;

confirming whether or not the authentication header of said frame is valid by using said extracted authentication header key;

searching said key management list table for said key management list containing the start-point terminal identifier of said frame when said authentication header is valid and the end-point terminal identifier of said frame is the terminal identifier of the corresponding terminal in order to extract said corresponding unicast encryption key; and

decrypting the payload of said frame by using said extracted unicast encryption key.

14. An encryption method for use in a terminal having a key management list table having at least one key management list for holding authentication header keys with respect to other terminals in such a manner as to correspond

to the terminal identifiers of the other terminals, said encryption method comprising the steps of:

searching said key management list table for said key management list containing the reception terminal identifier of a frame to be transmitted in order to extract said corresponding authentication header key;

generating a keyed hashed value, in which said extracted authentication header key is hashed together with a predetermined area of said frame, and giving the keyed hashed value as an authentication header to said frame; and

transmitting said frame.

15. A terminal management method for use in a terminal having a neighboring terminal list table for holding terminal identifiers of other terminals with which direct communication is possible among the terminals which form a network and a key management list table having at least one key management list for holding an authentication header key with respect to another terminal in such a manner as to correspond to the terminal identifier of the other terminal which forms said network, said terminal management method comprising the steps of:

detecting a leaving from said network at the terminals whose terminal identifiers are held in said neighboring terminal list table;

deleting from said key management list table said key management list containing the terminal identifier of the terminal that has left the network; and

transmitting a terminal leaving message informing the terminal identifier of said terminal that has left the network to the other terminals which form said network.

16. A terminal management method for use in a terminal having at least one key management list for holding authentication headers with respect to other terminals in such a manner as to correspond to the terminal identifiers of the other terminals which form the network, said terminal management method comprising the steps of:

receiving a terminal leaving message informing the terminal identifier of a terminal which has left said network; and

deleting from said key management list table said key management list containing the terminal identifier of said terminal which has left said network.